HONG KONG'S SUBMISSION TO
PRIVACY PROTECTION IN THE APEC ECONOMIES
MAPPING EXERCISE

APEC ELECTRONIC COMMERCE STEERING GROUP

FRAMEWORK FOR DATA PRIVACY

LEGAL PRIVACY INFRASTRUCTURE

1(a) Do you have any national laws relating to the protection of privacy and personal data by the government or the private sector? If not, are any such laws in development?

~ **Yes. The Personal Data (Privacy) Ordinance PD(P)O was enacted on 3 August 1995. The Office of the Privacy Commissioner for Personal Data was established on 1 August 1996 and the PD(P)O came into effect on 20 December 1996.**

~ **Under the PD(P)O personal data is defined as – any data**

(a) relating directly or indirectly to a living individual;
(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
(c) in a form in which access to or processing of the data is practicable.

1(b) If you do have national laws relating to the protection of privacy and personal data, please indicate if they are omnibus laws, general framework legislation subject to specific implementation by public authorities, or a combination of these approaches. Are any of these applicable laws available on a Web site? If so, please provide the URL(s).

~ **The provisions of the PD(P)O pertain to "data users" and "data subjects." In relation to personal data a data user means a person who, either alone or jointly or in common with other persons, controls the collection, holding and processing or use of the data. In relation to personal data, a data subject means the individual who is the subject of the data.**

~ **The PD(P)O is an omnibus law. It applies to individuals and all organisations irrespective of size, purpose and function in both the private and public sectors. Jurisdiction is restricted to the HKSAR.**

~ **The PD(P)O can be read at:**

http://www.pco.org.hk/english/ordinance/ordfull.html

1(c) Do these laws differentiate between requirements that are applicable to government versus those that deal with private sector collection of information,

and/or do separate laws or regulations apply to government collected personal data?

~ **No. The provisions of the PD(P)O do not discriminate in any way e.g. in favour of SME's or organisations with a stated minimum turnover etc.**

1(d) Are there are any privacy rights inherent in any laws, though not the subject of such laws?

~ The HKSAR is signatory to a number of international covenants e.g. The International Covenant on Economic, Social and Cultural Rights. Article 17 of the ICESCR makes a general reference to the privacy of the individual.

~ The Basic Law of Hong Kong and the Bill of Rights also make general reference to the privacy of the individual.

2 Do you have other legal regulations or guidance on the protection of privacy and personal data (such as administrative rules or regulations, decrees, ordinances, case law or other jurisprudence)? If not, are any such legal regulations in development?

~ **As the PD(P)O is a relatively new piece of legislation the body of case law pertaining to its interpretation is, of this date, very limited. However, there have been several important rulings and these have assisted the Office of the Privacy Commissioner in clarifying the interpretation placed upon certain provisions by the judiciary.**

~ **The Law Reform Commission in Hong Kong has a sub-committee on privacy that has issued a number of consultation papers on privacy-related issues e.g. Civil Liability for Invasion of Privacy (August 1999) and The Regulation of Media Intrusion (August 1999). However, final reports on these papers have yet to be issued. The consultation papers can be read at:**

<http://www.info.gov.hk>

~ **The HKSAR has committed to a privacy regimen that is characterised by an independent regulatory body - The Office of the Privacy Commissioner for Personal Data, supplemented by a statutory framework - The Personal Data (Privacy) Ordinance.**

~ Decisions of the Privacy Commissioner may be legally challenged in the courts or subject to review by the Administrative Appeals Board.

3 How and to what extent do laws and regulations identified in questions 1-2 affect the ability to transfer data across your national borders?

~ **Section 33 of the PD(P) O makes provision for:**

Prohibition against transfer of personal data to place outside Hong Kong except in specified circumstances.

~ **The provision* reads as follows:**

(1) This section shall not apply to personal data other than personal data the collection, holding, processing or use of which -
- **(a) takes place in Hong Kong; or**
- **(b) is controlled by a data user whose principal place of business is in Hong Kong.**

(2) A data user shall not transfer personal data to a place outside Hong Kong unless -
- **(a) the place is specified for the purposes of this section in a notice under subsection (3);**
- **(b) the user has reasonable grounds for believing that there is in force in that place any law which is substantially similar to, or servers the same purposes as, this Ordinance;**
- **(c) the data subject has consented in writing to the transfer;**
- **(d) the user has reasonable grounds for believing that, in all the circumstances of the case -**
  - **(i) the transfer is for the avoidance or mitigation of adverse action against the data subject;**
  - **(ii) it is not practicable to obtain the consent in writing of the data subject to that transfer; and**
  - **(iii) if it was practicable to obtain such consent, the data subject would give it;**
- **(e) the data are exempt from data protection principle 3 by virtue of an exemption under Part VIII; or**
- **(f) the user has taken all reasonable precautions and exercised all due diligence to ensure that the data will not, in that place, be collected, held, processed or used in any manner which, if that place were Hong Kong, would be a contravention of a requirement under this Ordinance.**

(3) Where the Commissioner has reasonable grounds for believing that there is in force in a place outside Hong Kong any law which is substantially similar to, or serves the same purposes as, this Ordinance, he may, by notice in the Gazette, specify that place for the purposes of this section.

(4) Where the Commissioner has reasonable grounds for believing that in a place specified in a notice under subsection (3) there is no longer in force any law which is substantially similar to, or serves the same purposes as, this Ordinance, he shall, either by repealing or amending that notice, cause that place to cease to be specified for the purposes of this section.

(5) For the avoidance of doubt, it is hereby declared that –
- **(a) for the purposes of subsection (1)(b), a data user which is a company incorporated in Hong Kong is a data user whose principal place of business is in Hong Kong;**

(b) a notice under subsection (3) is subsidiary legislation; and
(c) this section shall not operate to prejudice the generality of section 50.

~ ***NB This provision of the PD(P)O is the only provision that has yet to come into effect.***

4 Do the laws and regulations identified in questions 1-2 pertain to off-line data as well as to on-line data? Please describe the type(s) of data to which the laws and regulations identified in questions 1-2 apply. For example, do they apply to human resources or consumer data?

~ **Yes. The Office of the Privacy Commissioner for Personal Data upholds the personal data privacy principle that "what is illegal off-line is illegal on-line." This principle is applied by the PCO to any data user who collects personal data online.**

~ **The PD(P)O relates to all manifestations of personal data as defined in Q1(a) which would include human resource records, medical records and consumer data. Having said that the PD(P)O does allow for certain exemptions. The exemptions are contained in Part VIII of the Ordinance.**

5 What entities, organizations or persons are responsible for developing, implementing, monitoring and enforcing the laws, regulations, and policies related to privacy and personal data identified in questions 1-2?

~ **The Privacy Commissioner is responsible for upholding the provisions of the PD(P)O, ensuring compliance with those provisions and formulating policy regarding personal data privacy issues.**

~ **Under Section 50 of the PD(P)O the Privacy Commissioner may issue an Enforcement Notice if, after conducting an investigation, he is of the opinion that a data user has contravened a requirement of the PD(P)O.**

~ **The Office of the Privacy Commissioner is not empowered to prosecute cases where there appears to be just cause. Possible prosecutions are referred to the Department of Justice of the HKSAR government for their consideration.**

~ **The Office of the Privacy Commissioner for Personal Data is accountable to the Home Affairs Bureau ("the HAB") of the HKSAR government but only insofar as finance and accounting matters are concerned. Although funded by the HKSAR government it is important to recognise that the PCO is an independent statutory body.**

~ **Amendments to the provisions of the PD(P)O are proposed by the Legal Director or the Privacy Commissioner. These proposals are then referred to**

the Department of Justice for legal advice and drafting. Upon completion of drafting the government may draft an amendment bill to the PD(P)O for submission to the Legislative Council.

6 How does each entity, organization, or person identified in question 5 implement or enforce the laws and regulations references in questions 3-4? For example: through encouraging voluntary compliance, codes of conduct and other self-regulatory means? Through the promulgation of regulations or guidance? Through consumer and business education? Through the issuance of administrative, civil, or criminal order, including injunctive relief, fines, or penalties? Through monetary compensation (redress) for injured parties?

~ **The Office of the Privacy Commissioner for Personal Data uses a variety of strategies to encourage data users to comply with the provisions of the PD(P)O and to make data subjects aware of their personal data privacy rights. As an operating rule the PCO is committed to a strategy that favours persuasion over punishment. The belief is that an effective communications strategy supplemented by training seminars, public presentations and policy decisions that strike a balance between sectoral interests are the most effective means of encouraging compliance and disseminating personal data privacy rights.**

~ **The following list is indicative of the means by which the PCO seeks to achieve its objectives.**

- ~ **Complaints handling mediation of those complaints that meet prima facie requirements.**
- ~ **Inspection of systems, procedures and audits of personal data stored and processed by electronic means.**
- ~ **Publishing information brochures, FactSheets, procedural guidelines and handbooks on specific topics of contemporary interest e.g. E-Privacy.**
- ~ **Issuing Codes of Practice e.g. Identity Card Number and Personal Identifiers, Consumer Credit Data and Human Resource Management.**
- ~ **Announcements of Public Interest on local TV.**
- ~ **Press releases, press conferences, road shows and public relations campaigns.**
- ~ **Establishment and regular meetings of the Hong Kong Data Protection Officers Club. Current membership is in excess of 450 members drawn from all sectors of the economy.**
- ~ **Close liaison and consultation with representatives of interest groups e.g. professional institutes, employers, statutory bodies etc.**

7 To what extent are violations of the privacy laws and regulations identified in

questions 3-4 made publicly available? What organization, entity, or person is responsible for such publicity and how is it generally accomplished?

~ **Insofar as the transfer of personal data across national borders are concerned the provision regulating this activity is already contained in the PD(P)O. As explained, this is the only provision in the Ordinance that has yet to be enacted.**

~ **A contravention of the provisions contained in Section 33 may result in the Commissioner conducting an investigation into the nature of that contravention. Upon conducting an investigation, if the Commissioner were to find that there had been a contravention, or were to identify circumstances that would lead him to believe that the contravention may continue or be repeated then, under Section 50 of the Ordinance, he is empowered to issue an Enforcement Notice. Non-compliance with the conditions of an Enforcement Notice may result in the imposition of a fine.**

~ **Although the consequences of contravening any of the provisions of the PD(P)O are clearly specified in the Ordinance the PCO does not publicize the penalties that may be levied as a result of contravening Section 33 or other provisions of the Ordinance.**

~ **Insofar as online compliance with the provisions of the Ordinance are concerned the PCO conducts regular random checks on data subjects that collect personal data online. These checks seek to ensure that providers clearly display, or provide links to, their Personal Information Collection Statement ("PICS") and their Privacy Policy Statement (PPS).**

~ **A PICS is a statement given in compliance with the provisions of the PD(P)O that notifies data subjects of certain matters when collecting personal data from them. That is, it is a statement of a certain limited content given in relation to specific collections of recorded information from individuals about themselves.**

~ **A Personal Policy Statement is a general statement of an organisation's policy and practices in relation to its collection, holding and use of recorded information about individuals. Under the Ordinance, organisations are required to ensure that their policies and practices in this regard can be ascertained by other persons.**

~ **Where random checks of data users who collect personal data online reveal any shortcomings in terms of the Ordinance the PCO draws this to the attention of the website host. The site is issued with a notice informing it of the shortcomings identified and the steps that should, in a specified period of time, be taken to rectify matters. Once that period of time has elapsed the PCO will revisit the site to ensure that it is compliant with the provisions of the Ordinance and has clearly displayed a PICS, PPS and appropriate links. Where that is not the case the site is issued with an instruction to comply, within a specified period of time, and the possible consequences of failing to comply within that instruction.**

~ **The PCO have published a handbook titled Preparing Online Personal Information Collection Statements and Privacy Policy Statements, which is available at http://www.pco.org.hk/english/publications/pics_1.html.**

~ **The PCO is largely responsible for such publicity although media campaigns tend to place emphasis on the positive. The PCO has a Promotion and Training Manager and six staff that are responsible for administering the Communications and PR budget. As indicated in the response to question 6 the PCO's Communications Plan draws upon a number of strategies e.g. above and below-the-line, and ad hoc tactics to disseminate the messages it wishes to convey to the community.**

8 Are there cases of enforcement of privacy laws in your economy? If so, please provide some illustrative examples.

~ **Where there is prima facie evidence of a contravention of the PD(P)O the Privacy Commissioner is empowered, under Section 50, to conduct an investigation of the nature of the alleged contravention. If, upon conducting an investigation, the evidence substantiates a contravention of the Ordinance the Commissioner is empowered to issue an Enforcement Notice requesting the data user in question to refrain from any further contravention and/or put in place procedures that will prevent any further occurrence of the contravention.**

~ **If the terms and conditions of the Enforcement Notice are violated the Privacy Commissioner is empowered to pass the relevant documentation to the Department of Justice who may, on the legal merits of the case, decide to prosecute the data user. If the prosecution case is upheld by the Court the data user is liable, upon conviction, to an imprisonment of 6 months and a fine not exceeding HK$10,000 under Section 64 of the Ordinance.**

SELF REGULATION

9(a) In your jurisdiction, are there any private sector codes of conduct, guidelines, best practices or seal or trust mark programs relating to the protection of privacy or personal data that are endorsed by a business federation or widely used by the private sector? If so, please provide examples of entities, organizations or persons that are involved in these programs.

~ **The Codes of Practice issued by the PCO do not discriminate between the private and public sectors. They apply to all data users. The existing Codes of Practice, issued by the Office of the Privacy Commissioner for Personal Data, are available at http://www.pco.org.hk/english/publications/listofpub.html.**

~ **The Hong Kong Association of Accountants was licensed by WebTrust to**

launch, promote and ensure compliance with WebTrust standards in July 2000. As at the date of writing 8 organisations have signed up to the WebTrust programme in the HKSAR.

~ **The PCO has held discussions with Mobile Service Operators and produced a Guidance Note that outlines compliance requirements of the PD(P)O in relation to the practices of mobile service operators involved in the collection, use and processing of the personal data of mobile customer accounts. The Guidance Note is available at http://www.pco.org.hk/english/publications/guidance_mobile.html.**

~ **The PCO has held discussions with the Hong Kong Internet Service Providers Association ("HKISPA) regarding an Anti-SPAM Code of Practice. This Code of Practice, and related Implementation Guidelines, were launched in February 2000. The Code of Practice and the Implementation Guidelines are available at http://www.hkispa.org.hk/.**

~ **This Code of Practice does make provision for a branding scheme that is intended to inform the public about those websites that comply with its terms and conditions. Please refer to paragraph 8 of the Code of Practice which explains the branding scheme. At the time of writing it was not possible to verify with HKISPA the number of websites that had been authorised to display an icon informing visitors that the website is compliant with the terms of the Code of Practice.**

9(b) If not, are you aware of any efforts underway toward the development of such self-regulatory programs?

~ **Nil Return**

9(c) To what extent do organisations participate in these programmes or intitiatives?

~ **Involvement is best described as patchy, probably because data users regard the PCO as the authoritative voice on personal data privacy in the HKSAR and tend to look to it for guidelines and advice on compliance.**

~ **In 2000 the PCO launched a CD-ROM compliance kit titled Privacy. SAFE. This product was designed to assist data users in assessing whether their personal data management practices and procedures complied with the requirements of the Data Protection Principles ("DPP") and related provisions of the Ordinance. Another objective of Privacy.SAFE, was to provide a means for data users to perform self-monitoring privacy compliance within an organisation on an on-going basis.**

10 Are any of the initiatives identified in question 1(a) endorsed by a governmental entity? Is there a requirement that these programs be recognized by a governmental entity? Are any of them subject to government enforcement as a regulatory backstop?

~ **The Office of the Privacy Commissioner for Personal Data is an independent statutory body that is funded by the HKSAR government. Both the public and private sectors are expected to be compliant with the provisions of the PD(P)O. Under Section 12 of the PD(P)O the Privacy Commissioner is legally required to implement the following provision where a Code of Practice is concerned.**

"The Commissioner shall, before approving a code of practice under subsection (1) or any revision or proposed revision of the code under subsection (3), consult with –

(a) such bodies representative of data users to which the code or the code as revised, as the case may be, will apply (whether in whole or in part);

and

(b) such other interested persons."

~ **Openness and transparency are key aspects of the style of all government bureaux, departments and agencies of the Hong Kong government. The PCO is expected to apply that principle in terms of its dealings with the government, the Legislative Council and the general public.**

~ **The PCO is the first line of regulatory backstop for all personal data privacy issues regulated by the PD(P)O.**

11 Are there dispute resolution fora and mechanisms available for data privacy?

~ **Yes. When a data subject files a complaint with the PCO alleging that his/her personal data privacy rights have been infringed the complaint is screened against legal criteria to ensure that there is sufficient prima facie evidence to warrant a formal investigation of the complaint. Where that is so the case enters into the PCO's computer based Complaints Handling System ("CHS") and is assigned to staff of the Operations Division for investigation. This procedure is designed to filter out complaints that may be beyond the jurisdiction of the PCO or those that are trivial and vexatious.**

~ **In excess of 90% of bona fide complaint cases are successfully concluded through mediation between the parties to the complaint. Most complainants are satisfied with a verbal and/or written apology, and assurance that there will be no repetition of the cause giving rise to the complaint, where the data user is found to have infringed the privacy rights of the complainant.**

~ **Where a data subject is dissatisfied with the outcome of a complaint investigated by the Operations Division, he/she may inform the Privacy Commissioner accordingly. The complainant will then be informed that he/she may appeal any decision made by the PCO to the Administrative Appeals Board.**

~ **Insofar as the data user is concerned if, upon investigation, there is found to be a contravention of any of the provision(s) of the PD(P)O then section 50 empowers the Privacy Commissioner to take appropriate action. If, by the criteria established under section 50, there is subsequent evidence that the data user continues to contravene the Ordinance then the Privacy Commissioner is empowered to issue an Enforcement Notice. Non-compliance with an Enforcement Notice constitutes an offense under the Ordinance.**

~ **For the information of the general public the PCO has issued a leaflet titled Complaint Handling Policy, which is available at http://www.pco.org.hk/english/enquiries/complaint_handling.html.**

EDUCATIONAL EFFORTS

12 Are there any private sector, NGO, and/or governmental efforts to educate the public on their private rights? What entities, organizations, or persons are involved in these efforts?

~ **The Office of the Privacy Commissioner for Personal Data is largely responsible for educating members of the public about the rights conferred upon them by the provisions of the Ordinance. However, civil rights groups and other agencies of the government may, on occasion, inform the public of their privacy rights.**

~ **It is the intention of the Privacy Commissioner that, in future, the PCO make a concerted effort to target primary school children, secondary school and tertiary students with appropriate messages and information packs that will enable younger people to understand privacy and their personal data privacy rights.**

~ **Ultimately the Office of the Privacy Commissioner for Personal Data would like to see privacy rights included as a constituent element of a secondary school curriculum called Economics and Public Affairs. In part this curriculum tries to convey to students a sense of civic pride and responsibility. It also looks at some of the rights conferred upon individuals by the laws of Hong Kong.**

13 Are there any private sector, NGO, and/or governmental efforts to educate business about how to comply with the privacy laws and regulations listed in questions 1-2? What entities, associations, organizations, or persons are involved in these efforts?

~ **Again, educating the business community about the provisions of the Ordinance, and compliance with those provisions, is largely the role of the Office of the Privacy Commissioner. However, the PCO regularly works in conjunction with industry groups e.g. Chambers of Commerce and professional organisations e.g. the Hong Kong Institute of Human Resources. These are jointly sponsored forums that endeavour not merely to convey the work of the PCO but to apply the provisions of the Ordinance to a particular context. Both the Privacy Commissioner and Deputy Privacy Commissioner are very active in these programmes.**

14 What private sector, NGO and/or governmental guidance exists to assist companies in establishing private policies? What entities, organizations, or persons are involved in providing such guidance?

~ **Where non-PCO initiatives are taken in the private sector they are invariably sponsored by business groups, trade associations, employers' federations and professional institutes.**

~ **The PCO have, over the period of 5+ years of operation, directed considerable effort and resources to educating the private sector in terms of encouraging them to develop appropriate privacy policies, strategies and procedures designed to comply with the Ordinance.**

15 To what extent are technological solutions for privacy protection (privacy enhancing technologies or "PETS") used in your country by businesses and consumers? For example, security features, such as a firewall, encryption technologies, and/or privacy policy generators. Are there any efforts to educate the public about these technologies? If so, please provide examples of entities, organizations, or persons involved in these efforts.

~ **Many websites clearly indicate the IT measures that they have introduced to protect personal data submitted online. The PCO's view is that even though this may be so the public do not necessarily fully understand these measures which may well account for the reluctance in Hong Kong to shop online. That aside, it is not merely the technical system that needs to be made secure with safeguards (such as PETS) and appropriate operational protocols. It also needs to be recognised that the human side of the equation is equally important i.e. the character and integrity of staff entrusted to access databases containg large amounts of personal data.**

~ **However, it would generally be true to say that the emphasis in software applications still tends to be upon tracking and profiling website visitors rather than realising the value of PETS and Permission Marketing in allaying the fears of potential online consumers, notably in the B2C marketplace.**

ASSESSMENT

15 Are there any independent reports or government studies in your jurisdiction concerning the costs, benefits, or other effects of privacy laws and regulations and their enforcement?

~ **Not to the best of our knowledge. However, it is an informal policy of the PCO to convey to the business community in Hong Kong that although there are costs of complying with the provisions of the Ordinance the benefits outweigh the costs. Those benefits have been researched by the PCO and there is strong evidence from the business community that compliance with the provisions of the Ordinance brings long term benefits to the data user's organisation. The range of benefits identified are as follows:**

~ the public image of the organisation;

~ the management of personal data records;

~ the accuracy of personal data records;

~ customer/client relations; and

~ employee relationships.

16 Are there any studies in your jurisdiction concerning privacy self-regulation models or mixed models involving regulation with a law enforcement backstop?

~ **Not to the best of our knowledge.**

Office of the Privacy Commissioner for Personal Data
14 August 2002